Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/AU05/000487

International filing date: 04 April 2005 (04.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: AU
Number: 2004901799
Filing date: 02 April 2004 (02.04.2004)

Date of receipt at the International Bureau: 26 April 2005 (26.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/AU2005/000487

Australian Government

Patent Office
Canberra

I, JANENE PEISKER, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2004901799 for a patent by GREGORY ALAN COLLA as filed on 02 April 2004.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

WITNESS my hand this
Eighteenth day of April 2005

JANENE PEISKER
TEAM LEADER EXAMINATION
SUPPORT AND SALES

Method and Apparatus for the Operation of a Secure Email Gateway

Inventors: Gregory Alan COLLA, Neville Robert JONES

Field of Invention

The invention relates to method and apparatus for the operation of a secure email gateway.

Background to the Invention

E-mail is an essential business tool for the operation modern business. It provides an easily used tool for the transfer of information. Such information can be exchanged between people/machine and other people/machines.

A popular protocol for transferring e-mail is the Simple Message Transport Protocol (SMTP). This protocol is commonly used for the transport of messages between people and organisations across the Internet.

SMTP is prone to a number of security threats. Amongst these is the threat to message confidentiality. When a message is transmitted between the sender and recipient, it passes through many intermediate devices such as email relays and network routers. These devices may belong to any number of third parties. Each of these parties has the opportunity to access the contents of the message. Neither the sender nor the recipient may become aware that a third party has had access to, or made a copy of the message.

Further threats to message security are to its authenticity, integrity and non-repudiation. SMTP is a simple and open standard which has lead to email's popularity. However, its simplicity has made it possible for one entity to act as another, and so generating non-authentic messages. The recipient cannot tell the origins of the message, just from the message itself. Furthermore, if a message is modified en-route between the sender and recipient, the recipient will not be able to easily identify the modification. Finally, the sender of a message can repudiate its transmission.

To resolve these issues, messages security is required. Generally there are two solutions, secure networks and secure messages. Firstly, messages can be exchanged on secure networks, whereby confidentiality, authenticity, integrity and non-repudiation are assured to some degree. No specific security additions are required for the email client on these networks, as the environment is secure. Secondly, the message itself can be secured, and exchanged over an insecure network. This requires additional security features to the email client, so that they can generate and interpret secure messages.

Discussion of Prior Art

S/MIME

The intention of Secure Multipart Internet Mail Extensions (S/MIME) [RFC2311] is to secure messages between sender and recipient when transmitted across insecure networks.

S/MIME was developed in the late 90s and was the integration of a public key cryptosystem using trusted third parties with the MIME standard. S/MIME is based on RSA's PKCS#7 standard [PKCS#7].

S/MIME uses X.509 certificates [X.509] for electronic authentication of remote entities. The certificate contains a public key that is used to verify digital signatures and/or encrypt messages. The certficate also contains the entity's name and email address [RFC2312].

Generally, certificates are exchanged between parties in two ways. In the first mechanism, one party sends a signed message to the second. The signed message includes the sender's certificates. The second party can then use the public encryption key from the first party's certificate to generate an encrypted message for the first party. The second mechanism involves the publication of certificates in a directory which is accessible to other entities. One party retireve's a second party's certificates using a directory access protocol, eg Lightweight Directory Access Protocol (LDAP) [RFC2251] or using a web application connected with Hypertext Transfer Protocol [RFC2616]. Depending on the configuration of the directory, a remote user may be able to browse for certificates, or may be able to search for certificates, using the second party's email address, name, organisation, etc, as a serach index. The certificate retrieval mechanism is often a a feauture of secure email clients.

One problem identified with certificates published on publicly accessible directories is that they can be used as a tool for email address harvesting. It is possible for a third party to retrieve any number of certificates from the directory, and retrieve

associated users' email addresses. These email addresses can then be used for the transmission of unsolicted bulk email, also known as sapm.

Despite broad industry support for the standard the useability issues have inhibited S/MIME's adoption. The average end-user struggles to use the security features available to them and interoperability problems between S/MIME clients further exacerbates their frustrations. Obtaining a digital certificate from a trusted third party can also be a time consuming and costly process so there is resistance from potential recipients to bother getting a digital certificate in the first place.

S/MIME has been integrated into email clients such as Microsoft Outlook, Lotus Notes. It has also been implemented as a "plug-in" by third party developers, for example by Baltimore Technologies.

S/MIME has been integrated into secure email gateways. Email gateways join email networks. A secure email gateway gateway can be used to join a secure and an insecure network. On the secure network, the message travels "in-the-clear", as it does not require further security. On the insecure newtork, the message requires additional security, such as that available from S/MIME. The secure email gateway can act as a security proxy for entities on the secure network. The secure email gateway should be able to sign and/or encrypt messages crossing from the secure network to insecure network, and decrypt and/or verify messages crossing from the insecure network to the secure network. Secure email gateways remove the need for entities on secure networks to use and manage their own keys and encrypted email.

Problems associated with the operation of secure email gateways are the interoperability problems that they have with existing secure email clients, such as

those that comply with the S/MIME Certificate Handling protocol [RFC2312]. More specifically, when a secure email client verifies a message that is signed by a secure email gateway on behalf of another entity, it should warn the user that the signer's email address does not match the sender's email address. Furthermore, it is common for an email client to retrieve a recipient's encryption certficate in a directory by using the recipient's email address as the index. In the case of secure email gateway operation, the sender may not be able to retrive the email gateway's encryption certificate, as there is no standard mechanism to retrieve this from a directory, based on the recipient's email address.

Domain Security Services using S/MIME [RFC3183] defines a certificate profile for secure email gateways, gateway behaviour, and how secure email clients interoperate with these gateways. This does not resolve the two problems previously described, as it does not operate with existing secure email clients.

The S/MIME Certificate Handling protocol is being updated. The current draft [rfc2632bis-05] specificies that certificates that do not contain email addresses have no requirements for verifying the email address associated with the certificate. This does not resolve the problem of backwards compatibility with existing S/MIME clients, it degrades the security of message verification, and does not resolve the issue of encryption certificate retrieval.

PGP

Pretty Good Privacy (PGP) [RFC1991] was first developed in the early 1990s. It is a form of package security whereby a blob of data can be secured using public key

cryptography. When integrated with email software, PGP can simply take the content of an email message as its blob of data and secure it for the recipient of the message.

It has since become very popular with the Internet community because of its low price, ease of use and its simple 'web-of-trust' security model. However, there are scalability issues with the 'web-of-trust' model that limits its uptake in large communities.

Secure email gateways using PGP technology have been developed.

PEM

Privacy Enhanced Mail (PEM) was proposed in the mid-1990s and like PGP uses public key cryptography to secure an email message. It differs from PGP in that it uses a trusted third party security model to improve scalability. In this model a trusted third party issues the recipient's public key in the form of a digital certificate. Now the sender does not have to use a 'web-of-trust' to verify the recipient's public key before sending – they can simply verify that the trusted third party issued it.

PEM suffered from a case of bad timing. Just after it was released the Internet standard for defining how email messages could carry rich content like images, documents and so on was ratified (the MIME standard). PEM pre-dated this standard so it made it difficult to integrate the two. As a result PEM's useability suffered and was never really seen in the marketplace.

It is an object of the present invention to ameliorate problems with prior art solutions.

Table of Contents

Table of Figures

References

3DES	Data Encryption Standard, NIST, 1999, http://csrc.nist.gov/publications/fips/
milter	http://www.milter.org
mySQL	http://www.mysql.org
openbsd	http://www.openbsd.org
openldap	http://www.openldap.org
openssl	http://www.openssl.org
PGP	http://www.openpgp.org

PKCS#1	http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html
PKCS#7	http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html
RFC1939	Myers, et al, Post Office Protocol - Version 3, IETF, 1996, http://www.ietf.org/rfc/rfc1939.txt
RFC1991	Atkins, et al, PGP Message Exchange Formats, IETF, 1996, http://www.ietf.org/rfc/rfc1991.txt
RFC2251	Wahl, et al, Lightweight Directory Access Protocol (v3), IETF, 1997, http://www.ietf.org/rfc/rfc2251.txt
RFC2311	Dusse, et al, S/MIME Version 2 Message Specification, IETF, 1998, http://www.ietf.org/rfc/rfc2311.txt
RFC2312	Dusse, et al, S/MIME Version 2 Certificate Handling, IETF, 1998, http://www.ietf.org/rfc/rfc2312.txt
RFC2510	Adams, et al, Internet X.509 Public Key Infrastructure - Certificate Management Protocols, IETF, 1999, http://www.ietf.org/rfc/rfc2510.txt
RFC2616	Fielding, et al, Hypertext Transfer Protocol -- HTTP/1.1, IETF, 1999, http://www.ietf.org/rfc/rfc2616.txt
rfc2632bis-05	Ramsdell (ed), S/MIME Version 3.1 Certificate Handling - Internet Draft, IETF, 2003, http://www.imc.org/ietf-smime/index.html
RFC3183	Dean, et al, Domain Security Services using S/MIME, IETF, 2001, http://www.ietf.org/rfc/rfc3183.txt
RFC821	Postel, Simple Mail transport Protocol, IETF, 1982, http://www.ietf.org/rfc/rfc821.txt
sendmail	http://www.sendmail.org
sfl	http://digitalnet.com/knowledge/sfl_home.htm
SHA-1	Secure Hash Standard, NIST, 1995, http://www.itl.nist.gov/fipspubs/fip180-1.htm
X.509	The Directory: Public-key and attribute certificate frameworks, ITU, 2000, http://www.itu.int/home/index.html

Summary of the Invention

In accordance with an embodiment of the invention there is provided method and apparatus for the secure transmission of information.

In accordance with a further embodiment of the invention said information is transmitted via email from a sender to recipient or recipients.

In accordance with a further embodiment of the invention said email sender is connected to one network, and said email recipient is on a different email network. Said networks are connected with an email gateway.

In accordance with a further embodiment of the invention said email gateway is capable of securing messages prior to onwards delivery.

In accordance with a further embodiment of the invention there is provided method and apparatus for the provision of digital identifiers.

In accordance with a further embodiment of the invention said digital identifiers are provided by an Identification Provider.

In accordance with a further embodiment of the invention such digital identifiers are public key certificates [X.509][PGP].

In accordance with a further embodiment of the invention said Identification Provider generates said digital identifiers on demand.

In accordance with a further embodiment of the invention said Identification Provider caches digital certificates after they are generated.

In accordance with a further embodiment of the invention said Identification Provider accepts requests for said digital certificates using a directory access protocol.

In accordance with a further embodiment of the invention said Identification Provider accepts provides said digital certificates using a directory access protocol.

In accordance with a further embodimentof the invention said directory access protocol is the Lightweight Directory Access Protocol (LDAP) [RFC2251].

In accordance with a further embodiment of the invention said directory is accessible using Hypertext Transfer Protocol (HTTP) [RFC2616]

In accordance with a further embodiment of the invention said Identification Provider provides digital certificates that embed a network's email gateway public key.

In accordance with a further embodiment of the invention said Identification Provider provides digital certificates that embed an email address.

In accordance with a further embodiment of the invention said Identification Provider provides digital certificates that embed an email sender's email address.

In accordance with a further embodiment of the invention said Identification Provider provides digital certificates that embed an email recipient's email address.

In accordance with a further embodiment of the invention said Identification provider embeds any requested email address in said provided digital certificates.

In accordance with a further embodiment of the invention said gateway requests certificates from said Identification Provider.

In accordance with a further embodiment of the invention said gateway requests certificates from said Identification Provider using LDAP or the Certificate Management Protocol (CMP) [RFC2510].

In accordance with a further embodiment of the invention said gateway email signs message on behalf of a sender using said gateway's private key and attaching said certificate with sender's email address, whereby said public key embedded in said certificate can be used for message verification.

In accordance with a further embodiment of the invention said gateway public key can be used by a sending party for message encryption, whereby the sender retrieves the the gateway's public key from a certificate from the Identification Provider, indexed by the recipient's email address.

Detailed Description of the Invention

Description of System Deployment

The Secure Messaging System consists of the following components (refer Figure 1: System Deployment for Secure Email Gateway and On-Demand Certificate Authority).

(1) An insecure network. Messages on this network require further levels of security such as digital signatures and encryption, to be treated an authentic and confidential;

(2) A secure network. Cleartext messages on this network require no further security.

(3) A Secure Email Gateway that bridges the insecure (1) and secure (2) networks. The Secure Email Gateway has a public/private key pair used for message signing, and a public/private key pair for message encryption. The same key pair may be used for signing and encryption.

(4) A secure email client on the insecure network (1). The secure email client has the capability to encrypt and decrypt messages, as well as to sign and verify messages;

(5) An email client on the secure network (2);

(6) An "On-Demand Certification Authority" (ODCA), which is trusted by the secure email client (4), and produces certificates on behalf of entities on the secure network (5). The ODCA has access to the Email Gateway's public signing key and public encryption public key.

Intrinsic to the email network are email servers, email relays and domain name servers. These are used to transport the message from the sender to the recipient. The invention is described without these components.

Description of System Operation

Description of Message Signing by Secure Email Gateway

A user on the secure network (the sender) wishes to send a message to a user on the insecure network (the recipient). The sender wishes that the recipient be able to verify the authenticity of the message.

The sender generates the message using the email client on the secure network (Figure 1-5). The sender specifies the recipient's email address and sends the

message. The mail system on the secure network (Figure 1-2) routes the message to the Secure Email Gateway (Figure 1-3).

The Secure Email Gateway signs the message with its private signing key. It requests certificates for the sender from the On-Demand Certification Authority (Figure 1-6). The signing certificate has the Secure Email Gateway's public signing key and the sender's email address. The Secure Email Gateway attaches the signing certificate to the message. The Secure Email Gateway forwards the message to the recipient's email mailbox across the insecure network (Figure 1-1).

The recipient retrieves the message from the email mailbox using the secure email client on the insecure network (Figure 1-4). The secure email client verifies the authenticity of the message.

Description of Message Decryption by Secure Email Gateway

A user on the insecure network (the sender) wishes to send a message to a user on the secure network (the recipient). The sender wishes to ensure the contents of the message remains confidential.

The sender generates the message using the secure email client on the insecure network (Figure 1-4). The sender specifies the recipient's email address and specifies that the message is to be encrypted.

Prior to transmission, the secure email client (Figure 1-4) requests certificates for the recipient from the On-Demand Certification Authority (Figure 1-6). The encryption certificate contains the Secure Email Gateway's (Figure 1-3) public encryption key

and the recipient's email address. The secure email client uses the public key from the certificate to encrypt the message.

The secure email client transmits the encrypted message to the recipient.

The mail system on the insecure network (Figure 1-1) routes the message to the Secure Email Gateway .

The Secure Email Gateway (Figure 1-3) decrypts the message using its private decryption key. It forwards the decrypted message to the recipient.

The mail system on the secure network (Figure 1-2) routes the message to the recipient's mailbox. The recipient retrieves the message using the mail client on the secure network (Figure 1-5).

Description of Components

Description of Operation of the On-Demand Certification Authority

The On Demand Certification Authority consists of the following sub-components (refer Figure 2: Sequence diagram depicting operation of On-Demand Certification Authority):

(2) A directory access interface;

(3) A controller;

(4) A certification authority, with private signing key; and

(5) A database, which stores gateway certificates and caches generated certificates.

A requester (Figure 2-1) initiates the provision of certificates. The requester could be a secure email gateway or a secure email client.

The On Demand Certification Authority operates as follows (refer Figure 2: Sequence diagram depicting operation of On-Demand Certification Authority). For simplicity the provision of a single certificate is described, however generation of multiple certificates for various purposes is quite possible.

1. Request Certificate - (Figure 2-6)

   The requesting client (Figure 2-1) requests certificates from the On Demand Certification Authority via the directory access interface (Figure 2-2). It specifies the entity for which it requires certificates by the entity's email address.

2. Notify Controller - (Figure 2-7)

   The directory access interface (Figure 2-2) notifies the controller (Figure 2-3) of the request, including the entity's email address.

3. Retrieve Gateway Public Key - (Figure 2-8)

   The controller (Figure 2-3) uses the domain information from the email address as a key to retrieve the domain gateway's public key certificate from the database (Figure 2-5). The controller verifies the gateway's public key certificate and extracts the public key from the gateway certificate.

4. Generate Certificate (Figure 2-9)

   The controller (Figure 2-3) generates a public key certificate using the certification authority (Figure 2-4). It specifies that the public key is the one extracted from the

gateway's public key certificate, and that the email address is that of the requested entity.

5. Return Certificate to Controller (Figure 2-10)

The certification authority (Figure 2-4) returns the generated certificate to the controller (Figure 2-3).

6. Cache generated certificate ((Figure 2-11)

The controller (Figure 2-3) stores the generated certificate in the database (Figure 2-5).

7. Return Certificate to Directory Access Interface (Figure 2-12)

The controller (Figure 2-3) returns the generated certificate to the directory access interface (Figure 2-2).

8. Return Certificate to Requester (Figure 2-13)

The directory access interface (Figure 2-2) returns the generated certificate to the requesting client (Figure 2-1).

Preferred Implementation

INTERFACES AND PROTOCOLS

Request between Secure Email Gateway and On-Demand Gateway Certification Authority uses LDAP v2 [RFC2251] protocol.

Message transmission protocol is SMTP [RFC821]

Message retrieval protocol is POP3 [RFC1939].

Message security is provided with S/MIME [RFC2311].

Digital identifiers are X.509 v3 [X.509] certificates, with 1024 bit RSA [PKCS#1] keys.

Message digest is SHA-1 [SHA-1].

Message encryption is 3DES [3DES].

COMPONENTS

Email client is Microsoft Outlook Express 6, operating on a Microsoft Windows XP platform.

Secure Email client is Microsoft Outlook Express 6, operating on a Microsoft Windows XP platform.

Secure Email Gateway is sendmail 8.12.11 [sendmail] with custom S/MIME milter [milter]for message security that uses the S/MIME Freeware Library [sfl]. It operates using the openBSD 3.4 [openbsd] operating system on a Pentium 4 platform.

The On-Demand Certification Authority is customised using openSSL v9.7 [openssl] for the CA, openLDAP 2.2.8 [openldap] for the directory access interface and mySQL 4.0.18 [mySQL]for the database. It operates using the openBSD 3.4 [openbsd] operating system on an Intel Pentium 4 platform.

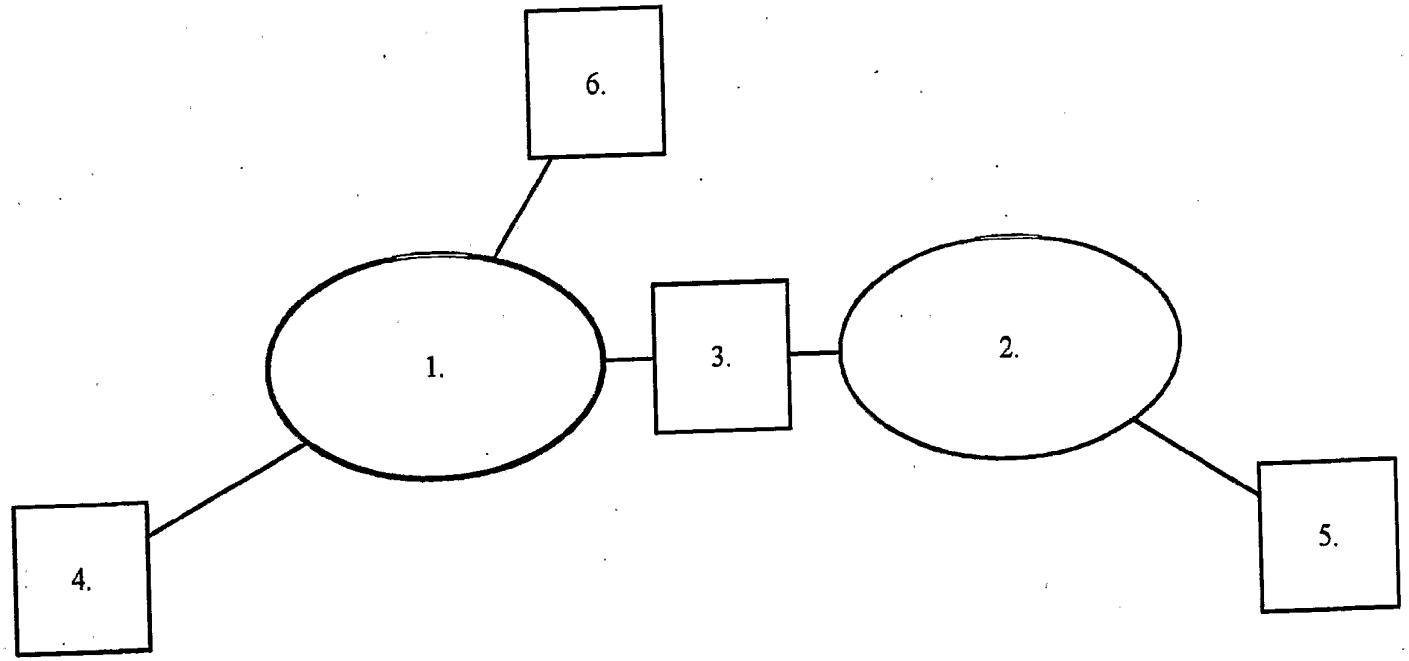

Figure 1: System Deployment for Secure Email Gateway and On-Demand Certificate Authority

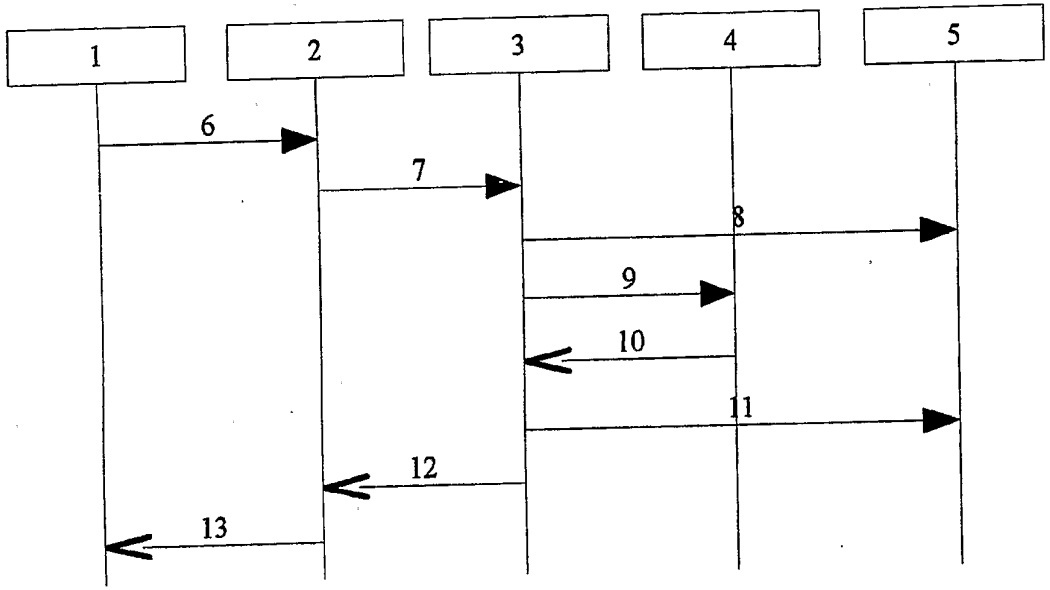

Figure 2: Sequence diagram depicting operation of On-Demand Certification Authority